(U//FOUO) OPSEC in SID - Some Answers

FROM: [redacted]
SID OPSEC Manager
Run Date: 01/12/2004

FROM: [redacted]
SID OPSEC Manager

(U//FOUO) By now everyone has heard about the President's visit to Iraq over Thanksgiving. This was a wonderful example of OPSEC in action, allowing the President to spend time with the troops safely. If we stop and take a look at all the work that goes on in SID, it's easy to see that each of us conducts equally sensitive, although less public, activities every day.

(U//FOUO) Last month we asked some questions about how OPSEC relates to SID employees (see previous article). This month we're going to answer those questions, and hopefully spark your interest to learn even more. The questions we asked were:

(U) How can you apply OPSEC in your day-to-day activities?

(U//FOUO) Given the wide variety of duties within SID, it would be impossible to give a detailed response applicable to every individual job. However, remember that OPSEC is a five-step process which can be applied to any position or job function:

- Step 1 - Identify your critical information. What is it that you do every day that an adversary would like to know? I challenge anyone to identify a position in SID that does not have at least one sensitive piece of information.

- Step 2 - Analyze the threat. Who cares about your information? Does that person or organization have the capability to obtain your information if it is not properly safeguarded?

- Step 3 - Identify vulnerabilities. Is there anything you do in your daily routine (inside or outside work) that could provide information to your adversary?

- Step 4 - Assess risk. If you have identified your critical information and determined that you have vulnerabilities in your routine, you're halfway there. Then consider your threat information. Does your adversary have the intent and capability to exploit your information? Do they intend to do harm to you or to your mission? Is there an impact to your mission if your adversary obtains your info? If you have a vulnerability, your adversary has intent and capability, and if there is impact to that vulnerability being exploited, you have risk.

- Step 5 - Apply countermeasures. Make a change to reduce your vulnerability or to lessen impact. This can be as simple as changing your phone call home to be "I'll be home late" rather than "Things are really crazy here since xxx happened. I'll be home once we finish yyyyy." (Fill in your own scenario for your office.)

(U) Where can you go if you have OPSEC questions or concerns?

(U//FOUO) There are OPSEC representatives throughout SID who should be able to respond to your questions, or at least point you in the right direction. Additionally, you can always contact the SID OPSEC Program Management team on [redacted] and we'll be glad to address any questions you may have.

(U) Whom can you contact to get more information, more training, or become more involved?

(U//FOUO) Additional OPSEC training is available through the Interagency OPSEC Support Staff ("go ioss" on the web). Additionally, with help from someone in your office, a SID OPSEC Program Manager can come to your organization and provide a tailored briefing on how OPSEC

applies to your particular job. One of the ways to get more involved is to volunteer to be an OPSEC representative for your work area. You'll get additional training and monthly updates on what is going on with SID OPSEC, as well as have a forum for discussing OPSEC concerns with other SID personnel.

(U) Is there more specific SID-applicable training on OPSEC?

(C) Yes! Very soon a brand new online class, OPSE-1201, titled "An Introduction to OPSEC for SID Personnel" will be available via VuPort. This course will step you through a real-world example of a SIGINT operation in a non-conventional location. You'll see an email announcing the course premiere shortly.

(U//FOUO) We hope we've answered some of your questions about OPSEC in SID. Look in SID *today* for future updates on our program and what it means to you. As always, if you have any questions relating to OPSEC issues, please contact your SID OPSEC Program Managers, [redacted] and [redacted] on [redacted]
